UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,869	08/31/2001	Luke D. Jagger	NAI1P025/01.156.01	2765

			EXAMINER
28875	7590	12/16/2004	JUNG, DAVID YIUK

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/944,869	JAGGER
	Examiner	Art Unit	
	David Y Jung	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any·reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _18 February 2002_.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-37_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-37_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _31 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _1/02_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-37 are presented.

CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed
> or described as set forth in section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are such that the subject
> matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was
> made.

Claims 1-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over

CNN (http://www-cgi.cnn.com/TECH/computing/9907/21/badrap.idg).

Regarding claim 1, CNN teaches "A method for preventing an outbreak of

malicious code, comprising: identifying malicious code at a local location on a network;

... information relating to the malicious code at the local location; sending the ...

information relating to the malicious code to a plurality of ... locations utilizing the

network; (the paragraph quoting Symantec, i.e. search for Back Orifice 2000, then

sending to researcher – this prevents the outbreak by identifying the Back Orifice 2000,

then sending information relating to Back Orifice 2000 which is a malicious code) and

blocking instances of the malicious code at the ... locations for a predetermined

moment of time based on the information; (the paragraph quoting Symantec, i.e.

quarantining) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code (the paragraph quoting Symantec, i.e. sending to researcher)."

These passages of CNN do not teach "remote" in the sense of the claim.

Nevertheless, it was well known in the art to reach a researcher at a remote location for the motivation of having access to expertise of a researcher that is not physically located on-site.

These passages of CNN do not teach "encrypted" in the sense of the claim.

Nevertheless, it was well known in the art to encrypt information for the motivation of hiding information from a hacker who appears to be using a malicious code to seize control of a system – such as in the situation of searching for Back Orifice 2000.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify CNN for the motivations noted in the previous paragraphs so as to teach the claimed invention.

Regarding claim 2 (handling virus, worm, Trojan, etc.), such particular features are well known in the art for the motivation of security. For example, CNN suggests handling a Trojan at the section quoting Symantec.

Regarding claim 3 (identification of source, etc.), such particular features are well known in the art for the motivation of security. For example, the Symantec's software noted in CNN would not even work unless such identification was possible. Regarding

claims 4-8, such particular features are well known in the art for the purpose of handling

information across computers.

Regarding claims 9, 10, these claims are computer program product analog

claim (claim 9) and system analog claim (claim 10) of claim 1. For the reasons noted in

the rejection of claim 1, these claims 9, 10 are not patentable.

Regarding claim 10, CNN teaches "A method for preventing an outbreak of

malicious code, comprising: identifying malicious code at a local location on a network;

information relating to the malicious code at the local location; sending the information

relating to the malicious code to a plurality of ... locations utilizing the network; (the

paragraph quoting Symantec, i.e. search for Back Orifice 2000, then sending to

researcher – this prevents the outbreak by identifying the Back Orifice 2000, then

sending information relating to Back Orifice 2000 which is a malicious code) and

blocking instances of the malicious code at the ... locations for a predetermined

moment of time based on the information; (the paragraph quoting Symantec, i.e.

quarantining) wherein the information is selected from the group consisting of a type,

context, protocol, severity, reporting server, and IP address associated with the

malicious code (the paragraph quoting Symantec, i.e. sending to researcher)."

These passages of CNN do not teach "remote" in the sense of the claim.

Nevertheless, it was well known in the art to reach a researcher at a remote

location for the motivation of having access to expertise of a researcher that is not

physically located on-site.

Hence, it would have been obvious to those of ordinary skill in the art at the time

of the claimed invention to modify CNN for the motivations noted in the previous

paragraphs so as to teach the claimed invention.

Regarding claims 11-36, such particular features are well known in the art for the

purpose of handling information across computers.

Regarding claim 37, CNN teaches "A method for preventing an outbreak of

malicious code, comprising: identifying malicious code at a local location on a network;

wherein the malicious code is at least one of a virus, worm and, Trojan; wherein the

malicious code is recognized based at least in part on recognizing that at least one of a

checksum and a file name of the malicious code is registered as a known threat; ...

information relating to the malicious code at the local location, wherein the information is

selected from the group consisting of a type, context, protocol, severity, reporting

server, and IP address associated with the malicious code; sending the ... information

relating to the malicious code to a plurality of ... locations utilizing the network; (the

paragraph quoting Symantec, i.e. search for Back Orifice 2000, then sending to

researcher – this prevents the outbreak by identifying the Back Orifice 2000, then

sending information relating to Back Orifice 2000 which is a malicious code) restricting

access to the ... locations by communications originating at the source of the malicious

code for a predetermined moment of time based on the information; (the paragraph

quoting Symantec, i.e. quarantining) executing countermeasures for limiting the effect of

the malicious code at the local location; and retrieving additional information about the

malicious code if an aspect of the attack is not recognized (the paragraph quoting

Symantec, i.e. sending to researcher)."

These passages of CNN do not teach "remote" in the sense of the claim.

Nevertheless, it was well known in the art to reach a researcher at a remote

location for the motivation of having access to expertise of a researcher that is not

physically located on-site.

These passages of CNN do not teach "encrypted" in the sense of the claim.

Nevertheless, it was well known in the art to encrypt information for the

motivation of hiding information from a hacker who appears to be using a malicious

code to seize control of a system – such as in the situation of searching for Back Orifice

2000.

Hence, it would have been obvious to those of ordinary skill in the art at the time

of the claimed invention to modify CNN for the motivations noted in the previous

paragraphs so as to teach the claimed invention.

Conclusion

The art made of record and not relied upon is considered pertinent to applicant's

disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 746-7239, (for formal communications intended for entry)

Or:

(703) 746-5606 (for informal or draft communications, please label "PROPOSED" or

"DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive,
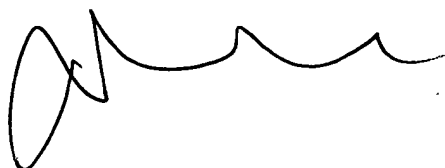
Arlington. VA., Sixth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to David Jung whose telephone number is (571) 272-3836

or Greg Morse whose telephone number is (571) 272-3838.

David Jung

Patent Examiner

12/13/04